Anexo

Especificación de Requerimientos de Seguridad en los contratos

Versión *8.00*

Gcia. Seguridad de la Información

Telefónica Argentina

Realizado por	Revisado por	Aprobado por
Diego Arias / Planificación y Tecnología de IT	*Malena Digon / Transformación de Seguridad*	*Paulo Escaño / Jefe Transformación de Seguridad*
18/01/2016	*14/03/2022*	*15/03/2022*

INDICE

1 CONTROL DE CAMBIOS

1.1 Control de cambios del Documento:

Versión	Fecha entrada en vigencia	Fecha fin de vigencia	Cambios realizados en versión	Responsable de definición de cambios
01.00	15/04/2013	19/02/2015	Versión Inicial	Nestor Perelman
02.00	19/02/2015	22/01/2016	Actualización de versión de NCSI y se suprimen los epígrafes que mención a la NCSI por el detalle de los requisitos	Nestor Perelman
03.00	22/01/2016	20/04/2018	Agregado de requisitos de servicios Cloud y Mobile	Diego Arias
04.00	20/04/2018	14/05/2018	Revisión y corrección completa del documento.	Malena Digon
05.00	14/05/2018	01/11/2018	Se modificó texto bajo los títulos de: "Arquitectura de Seguridad" y "Auditoria y Trazabilidad"	Malena Digon
06.00	01/11/2018	03/06/2019	Actualizado: - Objetivo - Roles y responsabilidades - Cloud	Miguel Olaya
07.00	03/06/2019	14/03/2022	Actualizado: - Arquitectura de Seguridad - Accesos lógicos - Cloud - Mobile - Desarrollo y Mantenimiento	Malena Digon / Miguel Olaya
08.00	14/03/2022	-	Se realizo una revisión completa del documento y se actualizaron todas las secciones.	Malena Digon / Diego Arias / Pablo Benedetti

1.2 Control de cambios del template:

Versión	Fecha entrada en vigencia	Fecha fin de vigencia	Cambios realizados en versión	Responsable de definición de cambios
01.00	15/07/2013	21/11/2014	Versión Inicial	Paula Trotta, Procesos y Calidad TI
01.01	21/11/2014	-	Agregado de tabla de roles y responsabilidades en Inciso 6. Agregado del control de cambios del template	Gabriela Moroz, Procesos y Calidad TI

2 OBJETIVO

El objetivo de este documento es realizar una descripción general de los requerimientos de seguridad que deberán ser tenidos en cuenta por el oferente al ser contratado el servicio y/o comprado, y que serán de cumplimiento obligatorio.

Dichos requerimientos se encuentran alineados con el Marco Normativo Corporativo de Seguridad de la Información de Telefónica Global. Siendo el cumplimiento de este marco obligatorio para todas las operadoras del grupo.

Así mismo, este documento debe ser utilizado solo en el marco contractual del servicio. Una vez finalizado este proceso, internamente se definirán los requerimientos de seguridad de manera precisa y detallada a cumplir en el desarrollo del servicio, en base al documento interno del "Catalogo de Requerimientos de Seguridad para Aplicaciones" y las consideraciones que defina en analista de Seguridad de la Información asignado. Por lo cual, este documento debe ser tomado como lineamientos generales estableciendo un marco y alcance de los requerimientos de seguridad de la información a nivel compañía.

3 ALCANCE

La definición del alcance y forma de cumplimiento de los requerimientos aquí indicados se realizará mediante el criterio que Telefónica considere, luego del análisis de riesgos correspondiente que definirá los niveles de acuerdo de servicio (SLA) indicados en estos requerimientos.

4 CONSIDERACIONES ESPECIALES

Telefónica se reserva el derecho de realizar auditorías y revisiones a los sistemas involucrados en el presente contrato, en los intervalos que considere.
Todos los desvíos a los requerimientos de este anexo se deberán corregir en un plazo definido (SLA), sin costo adicional para Telefónica y todo lo no consultado por fuera de este documento se define que será cumplido por el proveedor.

El contenido expresado en este documento debe ser considerado como confidencial entre las partes, por lo cual no debe ser divulgado a terceros y debe ser mantenido bajo la más estricta confidencialidad.

5 ABREVIATURAS Y DEFINICIONES

- **SLA**: Service Level Agreement. Acuerdo de nivel de servicio

- **SOX**: Ley Sarbanes-Oxley
- **PCI**: Payment Card Industry Data Security Standard. Estándar de Seguridad de Datos para la Industria de Tarjeta de pagos.
- **LDAPS**: Protocol ligero de acceso a directorios (LDAP) sobre SSL.
- **SSL**: Secure Socket Layer. Capa de conexión segura
- **DoS**: Denegación de servicios. Es un ataque que busca que un recurso no esté disponible para usuarios legítimos.

6 REFERENCIAS

Política Global de Seguridad

https://intranet.telefonica.com/normativa-grupo-telefonica/es/documento/politica-global-de-seguridad/

Normativa Global de Seguridad

https://intranet.telefonica.com/normativa-grupo-telefonica/es/documento/normativa-global-de-seguridad/

7 ROLES Y RESPONSABILIDADES

Seguridad de la Información

- Realizar análisis de riesgo y definir SLA en caso de que se requiera
- Establecer los diferentes controles que cubran los procesos y procedimientos que la compañía debe implementar, así como los que deben ser implementados por los proveedores.
- Gestionar la readecuación de los acuerdos en medida que se suscriben modificaciones tanto en alguna de las compañías del Grupo Telefónica como en sus proveedores.

Proveedor

- Cumplir los requerimientos definidos en este anexo en su producto y servicio.
- Cumplir con la Normativa de Gestión de Proveedores
- Aceptar, firmar y cumplir con el acuerdo de confidencialidad y no divulgación de la información durante la prestación de sus servicios y mantener dicha confidencialidad una vez finalizado el contrato.

Jefaturas / Gerencias

- Exigir el cumplimiento los requerimientos definidos en este anexo en su producto y servicio.
- Exigir el cumplimiento con la Normativa de Gestión de Proveedores

8 REQUERIMIENTOS

8.1 Consideraciones generales

1) Para que la construcción, modificación u operación de un aplicativo sea segura se requiere el conocimiento y la implementación de los tres pilares básicos de seguridad informática:
    a) Confidencialidad: se permite el acceso a los recursos solo a los usuarios autorizados.
    b) Integridad: los datos no puedan ser alterados o manipulados por usuarios no autorizados o por funcionamientos incorrectos de la aplicación.
    c) Disponibilidad: los sistemas y los datos deben estar disponibles a los usuarios autorizados siempre que sean requeridos.
2) Los principios de seguridad deben ser tenidos en cuenta en todas las etapas del ciclo de vida del proyecto: diseño, desarrollo, implementación y operación
3) Se debe dar protección frente a vulnerabilidades conocidas y ataques DoS.
4) Se debe implementar mecanismos capaces de detectar y frenar ataques de bots.
5) Se debe aplicar seguridad a todas las capas y elementos que intervienen en el sistema, desde la exposición del servicio hasta su consumo, así como en el código, control de versiones, arquitectura de red, sistema operativo, servidor web, servidor de aplicaciones, conexiones a bases de datos, colas, notificaciones, procesos, etcétera.

8.2 Marco Regulatorio

1) Deberá cumplir con los requerimientos definidos en la Normativa Corporativa de Seguridad de la Información de Telefónica y los procedimientos derivados de ella.
2) Deberá cumplir con los requerimientos normativos, legales y regulatorios tanto internos como nacionales e internacionales en función al tipo de información y/o servicios que estén alcanzados por la solución, sea el caso:
    a) Si maneja información financiera deberá cumplir con la Ley de SOX.
    b) Si maneja información de tarjetas de crédito o débito deberá ser PCI-DSS o PA.
    c) Si maneja información personal de empleados y/o clientes, deberá cumplir con la Ley de Protección de Datos Personales.

8.3 Acceso Lógico y Gestión de Identidades

1) El proceso de autenticación y autorización de la solución ofertada debe ser efectuado a través de la integración con los sistemas corporativos implementados bajo protocolos estándares (OAuth, SAML o Web Proxy) tanto para usuarios internos o clientes
2) La solución no deberá permitir el acceso simultáneo de un mismo usuario bajo la misma plataforma.
3) La solución deberá cerrar la sesión automáticamente luego de un determinado periodo de inactividad del usuario. El período debe ser configurable, con un máximo de 30 minutos.
4) La solución debe utilizar el mecanismo de control de acceso basado en perfiles (RBAC): Usuarios > Perfiles > Permisos.
    a) La asignación deberá ser por medio de la membresía/asignación de grupos perteneciente a la solución corporativa de identidades y accesos.
    b) Los roles deben ser creados bajo la condición de solo poder ver y/o gestionar lo requerido para el puesto.
    c) Todas las funcionalidades de la aplicación deben ser controladas por perfiles. No deben existir funcionalidades que exijan la configuración de atributos individuales por usuarios.
5) En caso de prestación de servicios por parte del proveedor, que requiera el acceso a los sistemas de Telefónica, el proveedor deberá:
    a) Designar un responsable gerencial y un responsable operativo que informará a Telefónica, por las vías formales definidas, los cambios de nómina que impacten en la asignación de privilegios en los sistemas de Telefónica, según el SLA definido.
    b) Segregar sus roles según los criterios y matrices de incompatibilidad de Telefónica. Por ejemplo: desarrollo, certificación, administración y soporte.
    c) Hacerse responsable por todas las acciones realizadas con los usuarios asociados a su contrato.
    d) Definir todos los usuarios personalizados. No se permitirá el uso de usuarios genéricos.
    e) Alinearse con los procedimientos definidos por Telefónica para el acceso remoto.
6) La solución no incluirá contraseñas en texto plano en ningún fichero binario.
7) La solución cifrará los tokens de autenticación en tránsito utilizando protocolos estándares y de última generación. Además, estos tokens expirarán al cierre de cada sesión quedando los mismo revocados y no pudiendo ser reutilizados.
8) La solución deberá almacenar la siguiente información como mínimo de los usuarios que acceden; ID de Usuario, nombre y apellido, DNI, correo electrónico, fecha de ultimo inicio de sesión correcto y perfil. Además, se deberá brindar un mecanismo que permita obtener esta información.
9) La solución deberá validar en cada pantalla que acceda un usuario que este cuente con los permisos para acceder a la misma.
10) La solución debe ser capaz de crear roles de acuerdo con el uso y administración de la aplicación. Asignado los permisos de los roles con lo mínimo que requiera para operar cada uno de ellos, y

separando los roles de Administración de Cuentas y Roles y de Administración de la aplicación (de existir ambos roles por necesidad de la solución).

11) La solución deberá asegurar que todos los usuarios tengan por lo menos un rol asociado.
12) La solución no permitirá el uso de usuarios genéricos (no personalizados) para tareas de operación o administración.
13) El proveedor deberá entregar documentación sobre el proceso de Gestion de Accesos y Acceso Lógico de identidades especificando en detalle de los roles, qué pantallas y accesos cuenta cada uno. Además, delegará toda la gestión de usuarios y roles a la compañía.
14) La solución no deberá permitir que se utilicen y generen cuentas de usuario locales a la misma.

8.4 Trazabilidad y Auditoria

1) La solución deberá registrar la auditoría de todas las transacciones definidas como críticas del sistema y las operaciones que realicen los usuarios en la aplicación tanto exitosas como fallidas.
2) La solución o el proveedor deberá suministrar mecanismos para el acceso y lectura de los registros de auditoría cuando sea solicitado por la compañía.
3) La solución deberá registrar los siguientes eventos, cuando estos se encuentren presentes:
   a) Inicio de sesión y cierre de sesión de usuarios. (Exitosos y Fallidos)
   b) Eventos del sistema.
   c) Gestión de cuentas de usuarios, roles y/o permisos
   d) Cambios en las configuraciones de la aplicación.
   e) Escalamiento de privilegios
   f) Acciones realizadas por las cuentas administrativas
   g) Eventos relacionados con la seguridad de la aplicación
   h) Fallas del sistema/aplicación
   i) Cambios en la activación/desactivación de auditoría de logs
   j) Mensajes de errores generados por la aplicación
4) En ningún momento los registros de auditoría creados por la aplicación deberán contener datos considerados confidenciales y/o sensibles.
5) Los archivos de registro deben almacenarse de forma segura y tener restricción de acceso, principalmente en los casos de permiso de cambio y eliminación. El acceso y la lectura de los archivos de registro deben restringirse a los usuarios autorizados.
6) El tiempo de retención de los registros de auditoria serán definidos por el área de Seguridad de la Información con un mínimo de 7 años.
7) Los registros de auditoría de los diferentes componentes de la solución deberán ser inequívocamente relacionados para asegurar la trazabilidad de las acciones realizadas.
8) La solución deberá almacenar por cada registro de auditoria la siguiente información:
   a) Sistema, aplicación o dispositivo que ha generado el registro

b) Identificador (login usuario, ID proceso, dirección IP, terminal, etc.) de la persona, programa o elemento que origina el evento que se registra
c) Fecha y hora en que se produce el evento
d) Descripción o motivo del evento que se registra: acceso, caída de un sistema, error que se ha producido, etc.
e) En caso de corresponderse con un evento de acceso:
    i) Recurso al que se accede (información, aplicación, red, disco, etc.)
    ii) Tipo de acceso (lectura, modificación, consulta, listado, borrado, etc.)
    iii) Si el acceso ha sido autorizado o no
    iv) Uso de privilegio
    v) Terminal o sistema desde el que se accede

9) Todos los componentes de la solución deberán estar sincronizados con el reloj definido por Telefónica.
10) La solución debe estar preparada para integrarse al SIEM de Telefónica.

8.5 Gestión de la Configuración

1) Se deberá cumplir con todos los requerimientos solicitados por la compañía que permitan aumentar el nivel de seguridad de la herramienta, solución o componente, en base a las configuraciones posibles de la misma.
2) Toda la infraestructura involucrada deberá cumplir en su totalidad con las plantillas de seguridad aplicadas y actualizadas tanto ~~como~~ para Sistemas Operativos y Base de Datos.
3) Deberá permitir la integración de los sistemas de control de configuración de Telefónica.
4) Deberá la solución ser compatible con la solución homologada de Antivirus de Telefónica.
5) Deberá la infraestructura que de~~n~~ soporte a la solución estar actualizada en su última versión, tanto de sistema operativo, base de datos o componentes de esta.
6) Deberá integrarse con los requerimientos y políticas de respaldo y recuperación de Telefónica, definido en el documento en referencia, y detalladas en procedimientos particulares.
7) Se deberá cumplir con un SLA definido por Telefónica, en función de la criticidad de la información y/o los servicios afectados, para la disponibilidad de parches propios de la solución u homologación de parches de terceros
8) Ningún componente y/o servicio de la solución debe requerir privilegios administrativos y/o de superusuario para su ejecución.

8.6 Arquitectura de Seguridad

1) Deben existir ambientes de Desarrollo, Certificación y Producción. Estos deben estar separados entre sí. El ambiente de certificación debe ser lo más similar posible al productivo (mismo

sistema operativo, web server, base de datos, configuración, bibliotecas, etc.) y debe estar disponible para que desde el área de seguridad se puedan realizar pruebas.

2) Las vulnerabilidades detectadas en los componentes del sistema deben corregirse dentro de la ventana de riesgo definida por Telefónica, en función de la criticidad de la información o los servicios asociados.
3) Toda interfaz web, sea aplicación o web service, deberá cumplir con los requerimientos definidos en OWASP (Comunidad Abierta sobre Seguridad en Aplicaciones) y las buenas prácticas para el desarrollo seguro.
4) Se deberá asegurar el correcto procesamiento de la información en las aplicaciones, cumpliendo con los siguientes requerimientos:
   a) Validación de datos de entrada: las entradas de datos en las aplicaciones deben ser validados previo a su procesamiento para asegurar que son correctos y apropiados.
   b) Control de procesamiento interno: Se deben incorporar las verificaciones de validación a las aplicaciones para detectar cualquier caso de corrupción de la información a través del procesamiento de errores o actos deliberados.
   c) Integridad de los datos: Se debe asegurar la autenticidad y la integridad de los datos de las aplicaciones.
   d) Validación de datos de salida: Se debe validar la salida de datos de la aplicación para garantizar que el procesamiento de la información almacenada sea correcto y adecuado a las circunstancias.
5) El sistema deberá proveer mecanismos para la protección de la información crítica que maneje en todas las etapas de su ciclo de vida (generación, tratamiento, transporte, almacenamiento y destrucción).
6) Deberá usar protocolos de acceso y transporte de información seguros, y no se utilizarán protocolos que presenten debilidades de seguridad.
7) Deberá proveer autenticación en las API o WS, si los hubiere.
8) Toda API o WS que interactúa con elementos externos al producto debe pasar por el API-GW corporativo.
9) Todos los componentes usados como soporte para brindar funcionalidad a la aplicación (ej.: bibliotecas de terceros) deben estar actualizadas a su última versión estable. De lanzarse una nueva versión el proveedor deberá confirmar la compatibilidad de esta con la aplicación y hacer los ajustes necesarios, si corresponden, para su uso.
10) Deberá permitir segregar la interfaz de gestión de la de servicio y aplicar listas de control de acceso para restringir el origen de las conexiones. Los orígenes deberán ser validados por el analista de seguridad de Telefónica.
11) Todo el tráfico de la solución debe ser protegido por HTTPS/TLS utilizando certificados digitales.

8.7 Cloud

1) Se debe cumplir con todo lo indicado en los puntos 8.1 al 8.6

2) Especificar la locación física de los datos, para que sean consideradas las legislaciones sobre el país residente de la información.
3) Revisar con el analista de Seguridad de la Información los requerimientos puntuales para el desarrollo en Cloud.
4) El proveedor debe cumplir con los controles del estándar internacional ISO 27002 en el ámbito del servicio y debe poseer y mantener en el tiempo una certificación de seguridad como ISO 27001 o SAS70 tipo II (SSAE 16) o similar.
5) El acceso físico a las instalaciones en las que se ubica la infraestructura clave debe estar adecuadamente controlado y restringido a las personas que lo necesitan.
6) Se deben contratar e informar al analista de Seguridad de la Información, los módulos de seguridad con los que cuente la nube que aseguren su acceso y uso.

8.8 Mobile

1) Se debe cumplir con todo lo indicado en los puntos 8.1 al 8.6
2) Se debe cumplir con los requisitos establecidos por el estándar OWASP. Además, se deben seguir las prácticas de desarrollo seguro acordes a la plataforma usada.
   a) IOS, IOS Security Development Checklists: https://developer.apple.com/library/ios/documentation/Security/Conceptual/SecureCodingGuide/SecurityDevelopmentChecklists/SecurityDevelopmentChecklists.html
   b) Android, Android Best Practices for Security & Privacy http://developer.android.com/training/best-security.html
3) No se debe almacenar información sensible en dispositivos móviles.
4) Si es necesario almacenar datos en el dispositivo móvil, por ejemplo, en caché, estos datos deben cifrarse con protocolos seguros.
5) No se deben almacenar claves de cifrado en dispositivos móviles.
6) La aplicación mantendrá en memoria las credenciales de acceso (contraseñas) el mínimo tiempo posible para completar el proceso de validación.
7) La aplicación utilizará los mínimos permisos necesarios para ejecutarse en el dispositivo.
8) La aplicación no abrirá puertos para escucha en el dispositivo cliente.
9) La aplicación avisará al usuario y obtendrá su consentimiento sobre las consecuencias financieras derivadas de la transacción solicitada.
10) La aplicación no estará autorizada a ejecutar código con privilegios de administración (root\system).
11) La aplicación se actualizará automáticamente en los dispositivos cuando sea necesario.
12) La aplicación implementará una configuración de usuario por defecto lo más segura posible (buscando un equilibrio entre seguridad y usabilidad).

13) La aplicación informará al usuario los posibles riesgos cuando se cambian los parámetros de seguridad en la configuración. En estos casos, la opción por defecto seleccionada debe ser la más restrictiva desde el punto de vista de seguridad.
14) La aplicación debe cargar plug-ins y extensiones solo desde orígenes seguros con acceso restringido.
15) La aplicación se distribuirá y actualizará a través de los portales y tiendas de aplicaciones oficiales (App Store, Google Play, etc.).
16) La aplicación ofrecerá canales de comunicación para que los usuarios puedan informar sobre problemas de seguridad que detecten en la aplicación (por ejemplo, e-mail).
17) La aplicación móvil no utilizará notificaciones del tipo SMS, MMS o similares para enviar datos sensibles desde/hacia los dispositivos móviles.
18) La aplicación no debe ser compatible sobre sistemas operativos obsoletos.

8.9 Big Data

1) Ante la necesidad de integración contra el entorno de Big data corporativo, el proveedor deberá cumplir con los estándares de la suite de CDP (Cloudera Data Platform), ex Hortonworks, y en sus nuevas versiones. Contemplando además la integración, administración, autenticación, autorización y protección de datos de auditoría.
2) Deberá cumplir con los estándares de anonimización y cifrado, tanto de la suite Hortonworks HDP en sus versiones 2.x como sus futuras versiones

8.10 Desarrollo y mantenimiento

8.10.1 Seguridad en el ciclo de vida del software

1) El proveedor deberá proporcionar la documentación que describa claramente el diseño realizado para cumplir con los requerimientos de seguridad especificados, tales como arquitectura y patrones de diseño propuestos.
2) El proveedor se compromete a contar con una metodología de desarrollo seguro, reconocida por la industria de software.
3) El proveedor se compromete a seguir buenas prácticas de codificación segura y utilizará, siempre que sea posible, bibliotecas comunes que proporcionen seguridad en la programación de interfaces (p.ej.: ESAPI de OWASP).
4) El proveedor se compromete a verificar el cumplimiento de los requisitos de seguridad antes de la entrega de producto, así como a compartir los problemas de seguridad encontrados.

5) El proveedor deberá establecer un modelo de certificación de la seguridad de su sistema consensuado con el cliente en cada una de sus etapas: ejecución, comunicación y remediación de vulnerabilidades.
6) El proveedor deberá proporcionar todas las opciones de configuración relevantes para la seguridad del producto y sus implicaciones, describiendo las dependencias entre las plataformas (sistema operativo, servidor web, base de datos, etc.).
7) El proveedor deberá comunicar al cliente sobre el resultado de los procesos de evaluación de riesgos tecnológicos de los componentes del sistema, procesos técnicos y funcionales soportados, colaborando, cuando así sea requerido, en su mitigación.
8) En el caso de subcontratación el proveedor se obliga a trasladar a la empresa subcontratada las mismas obligaciones que las asumidas por él en relación con la ejecución de los trabajos.

8.10.2 Entornos de desarrollo

1) El proveedor deberá especificar qué herramientas utiliza en el entorno de desarrollo de software para fomentar la codificación segura.
2) El proveedor debe utilizar un sistema de control del código fuente que permita autenticar a todos los miembros del equipo y registre todos los cambios realizados sobre la línea base, así como sobre los ficheros de configuración y compilación. Deberá garantizarse la integridad del software entregado. Este sistema de control del código fuente debe tener un control de versiones que incluya la documentación de los cambios realizados.
3) En caso de que el proveedor utilice entornos de desarrollo y pruebas o desarrollo fuera del control de la organización después de la prestación contractual estos ambientes deben ser eliminados completamente.
4) Se requiere que el proveedor utilice herramientas de integración continua para el despliegue entre ambientes y la ejecución de pruebas unitarias de los servicios a realizar. El ambiente debe estar preparado para dicho fin (desarrollo, testing).
5) Se requiere que el proveedor garantice la disponibilidad de la información proporcionada por el software de control de código, versión e integración continua.

8.10.3 Bibliotecas y productos de terceros

1) El proveedor se compromete a informar al cliente de todo el software de terceros utilizados durante el desarrollo, incluyendo bibliotecas, entornos, componentes, y otros productos, tanto comerciales como open-source. Para dichos componentes, el proveedor debe garantizar que éstos no tienen vulnerabilidades publicadas o conocidas en la industria.

8.10.4 Gestión de vulnerabilidades

1) El proveedor se compromete a rastrear los problemas de seguridad no cubiertos durante el ciclo de vida del desarrollo. El riesgo asociado a cada debilidad de seguridad será evaluado, documentado y reportado al cliente tan pronto como sea posible.
2) El proveedor será responsable de proteger la documentación acerca de las vulnerabilidades de seguridad, con el fin de limitar la probabilidad de que se produzca la exposición de dichas debilidades en el entorno productivo.
3) Las vulnerabilidades de seguridad que se identifiquen antes de la implementación deberán ser solventadas por el proveedor.
4) El proveedor del software deberá comprometerse a la mitigación de las vulnerabilidades reportadas atendiendo a la su criticidad (crítica: 48hs días, alta: 5 días hábiles).
5) El cliente puede en todo momento, o a la finalización de cada ciclo de vida del desarrollo, realizar los controles de vulnerabilidades del producto.
6) El proveedor deberá garantizar explícitamente que implementa un modelo de protección aplicable a sus empleados y colaboradores que asegura un nivel de seguridad suficiente en el acceso a redes, sistemas y datos de Telefónica. Dicho modelo de protección deberá ser entregado a Telefónica.

8.10.5 Garantía

1) El software no se considerará aceptado hasta que todos los problemas de seguridad se les haya sido asignados a un plan de acción validado por ambas partes.
2) El proveedor garantiza que el software no contiene ningún tipo de programa maligno, incluidos los virus informáticos, gusanos, bombas de tiempo, puertas traseras, troyanos, los huevos de pascua, así como todas las demás formas conocidas de código malicioso.
3) Las vulnerabilidades encontradas en el software que no sean consideradas como críticas, altas o de riesgo medio, se denominaran “warnings” (advertencias). Estos warnings no influirán en la aceptación de la entrega, pero sí que serán registrados para ser solventados en futuras versiones. Para los warnings en espera de ser solventados en futuras versiones, el proveedor deberá proporcionar parches o definir controles compensatorios de mitigación del riesgo de la vulnerabilidad.
4) Los “warnings” encontrados en la solución deben ser acompañados del correspondiente plan de acción con sus respectivas fechas de compromiso de remediación.

8.11 Respaldo y recuperación

1) Deberá definir y realizar resguardos de información en base al riesgo asociado al proyecto y lo que defina el Analista de Seguridad de la Información asignado. Se deberán tener en cuenta los siguientes puntos:
   a) Los responsables de realizar las copias de respaldo y posterior custodia.
   b) Periodicidad de las copias de respaldo.
   c) Número de copias.
   d) Tipo de respaldo (completa o diferencial/incremental).
   e) Tiempos máximos de almacenamiento (fecha de expiración) y si es necesario eliminar la información una vez alcanzada la fecha de expiración (así como el tipo procedimiento de destrucción exigido)
   f) Tiempos mínimos aceptables para recuperar de la información.
2) Se deberá cifrar la información respaldada en función de los siguientes aspectos:
   a) La naturaleza de la información (financiera, contratos con clientes, registros de accesos, sistemas operativos, etc.).
   b) Los requisitos de disponibilidad determinados por el Propietario de la información de acuerdo con las necesidades del negocio.
   c) Nivel de clasificación de la información.
   d) Los requisitos legales aplicables en cada país.
   e) Políticas internas de retención de información y datos.
   f) Los niveles de servicio acordados.
   g) Riesgo tecnológico implícito.
   h) Los planes de continuidad de negocio.
3) El proveedor debe generar los procedimientos de recuperación asociados.
4) Las copias de respaldo serán rotuladas e inventariadas, considerando la clasificación de la información.
5) Las claves de cifrado y programas asociados deberán guardarse de forma separada, de manera que se pueda recuperar la información a partir de la información cifrada en caso de ser necesario.
6) Las copias de respaldo se realizarán de manera que se pueda recuperar, de forma separada e independiente, el sistema y la información que procesa.
7) Las copias de respaldo realizadas se verificarán periódicamente y de forma rotativa de acuerdo con un plan de pruebas definido, utilizando una herramienta de verificación o restaurando parte del conjunto para garantizar que las copias estarán disponibles cuando sean necesitadas.
8) En los casos en los que sea posible, se debe automatizar el procedimiento de realización de copias de respaldo mediante programación periódica de las mismas.
9) En el caso de los datos sean de carácter personal sensibles, se deberá conservará una copia de respaldo de la información y copia de los procedimientos de recuperación en un lugar diferente de

aquél en que se encuentren los sistemas que tratan la información, que deberá cumplir en todo caso con las medidas de seguridad de la ubicación original, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

10) Se verificará periódicamente la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

8.12 Integración con la Red de la compañía

1) En base a los niveles de riesgo, el proveedor deberá tener en cuenta que se segregaran en varios segmentos lógicos y/o físicos la red donde resida la aplicación. Estos segmentos de red se aislarán mediante dispositivos, que controlarán el acceso y el tráfico entre los segmentos de acuerdo con los criterios y políticas definidas. La solución debe soportar la segregación en capas separando las zonas de presentación (DMZ) de las zonas de aplicación con el mínimo de apertura de puertos de comunicación en los firewalls entre las zonas. El proveedor debe cumplir con una mínima segregación de redes de gestión, tráfico y servicios internos o expuestos.
2) El proveedor deberá definir y cumplir con los siguientes requerimientos para conectarse con la compañía en base a lo defino por la empresa:
   a) Las personas responsables de autorizar las solicitudes (deberá estar involucrado el Analista de Seguridad de la Información).
   b) La forma de acceso de los usuarios a los segmentos de red, así como los posibles mecanismos de identificación, autenticación, control de accesos y registro de acceso.
3) El proveedor deberá considerar los siguientes puntos que serán requeridos por Telefónica:
   a) Todo está prohibido a menos que esté expresamente permitido.
   b) Evitar que los ataques que se produzcan desde el interior de un segmento de red afecten al resto (propagación de gusanos, etc.).
   c) Evitar los ataques de denegación de servicio en la medida de lo posible.
   d) Evitar la suplantación de direcciones origen.
   e) Permitir la gestión remota sólo desde ciertas direcciones autorizadas.
   f) Registrar los eventos de seguridad (logs) o garantizar los requisitos del negocio.
   g) Definir los diferentes niveles de riesgo de los segmentos de red de la aplicación.
4) El proveedor deberá utilizar la VPN de Proveedores para acceso a recursos de Telefónica. La autenticación de la VPN deberá ser conforma los estándares establecidos por compañía.
5) No se permitirá la conexión a redes externas directas en sistemas que estén conectados a la red interna.

6) Los pasos para solicitar, autorizar o anular la interconexión de la red interna de la empresa con redes externas, se indicarán en un procedimiento definido en el cual se identificará el responsable de otorgar las autorizaciones.